분산 서비스 공격 대응을 위한 역추적 시스템 개발

이직수*, 최병선, 이재광
*한남대학교 컴퓨터공학과
e-mail:jslee@netwk.hannam.ac.kr

Traceback System for DDoS Attack Response

Jik-Su Lee*, Byoung-Sun Choi, Jae-Kwang Lee
*Dept of Computer Engineering, Hannam University

요 약

컴퓨터와 네트워크의 보급이 일반화되면서 인터넷을 통한 정보 전달이 일상생활처럼 되고 있다. 또한 인터넷, 무선통신, 그리고 자료 교환에 대한 증가로 인해 다른 사용자와 접속하기 위한 방식은 빠르게 변화하고 있다. 그러나 기존의 침입 차단 시스템과 침입 탐지 시스템과 같은 시스템 외부방어 개념의 보안 대책은 전산망 내의 중요한 정보 및 자원을 보호함에 있어서 그 한계를 갖는다. 본 논문에서는 해킹으로 판단되는 침입에 대하여 라우터의 구조적 변경 없이 효율적으로 역추적 하기 위해서 ICMP 역추적 메시지(ICMP Traceback Message)를 이용한 ICMP 기반의 역추적 시스템을 설계한다.

1. 서론[1)]

최근 컴퓨터 기술의 발달과 인터넷의 발전으로 인해 업무 효율이 높아졌고 생활의 질이 높아졌다. 하지만 컴퓨터 기술과 인터넷 기술의 발전은 긍정적인 효과뿐만 아니라 외부 시스템의 불법 침입, 중요 정보의 유출, 서비스 거부 공격 등 역기능도 생겨났다.

이에 최근의 정보보호 관경에서는 자신의 관리 도메인 내로 침입하게 되는 공격을 어떻게 효율적으로 탐지할 것인가와 탐지된 공격을 어떻게 효율적으로 차단하여 자신의 도메인을 잘 보호할 것인가에 초점이 맞추어지게 되었다. 하지만 탐지된 침입에 대한 대응도 자신의 도메인 경계에서 해당 트래픽을 차단하는 수동적인 방법 이외에는 별다른 방법이 없는 상태이다. 그래서 자신의 도메인 입구에서만 해당 트래픽을 차단함으로써 침입자는 인터넷을 통하여 제2, 제3의 공격을 할 수 있게 된다. 인터넷을 통한 경제 활동이 점자 증가하는 요즘 사이버 공격으로 입는 피해는 기업의 생존을 위협하는 수준에 도달하게 되었다. 따라서 이러한 사이버 공격에 대한 능동으로 대응할 수 있는 기술이 요구된다고 할 수 있다. 이런 능동적인 대응의 가장 기본적으로 요구되는 기술이 공격자의 실제 위치를 파악하는 역추적 기술이라고 할 수 있다[1].

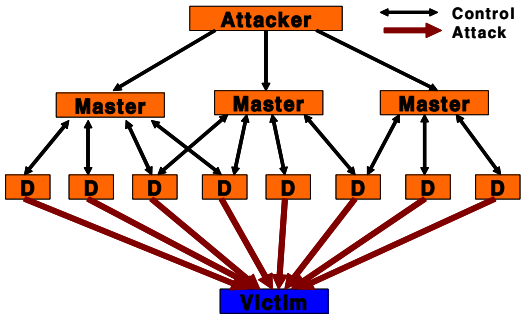
1) 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.

2. 관련연구

2.1 DDoS(Distributed Denial of Service)

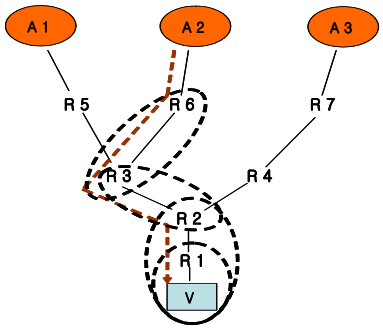
해킹 사건에 사용된 수법인 분산 서비스 거부공격(DDoS: Distributed Denial of service)은 마스터 서버에 접속하여 하나 혹은 여러 개의 IP 주소를 대상으로 서비스 거부 공격을 수행하게 된다. 이럴 경우 트리누 마스터는 특정한 기간에 하나 혹은 여러 개의 IP 주소를 공격하도록 하부 서버와 통신한다. 이는 공격자의 명령에 의해 공격 도구가 설치된 대량의 서버들을 제어해 공격 대상 시스템에 치명적인 서비스 거부 공격을 수행하기 때문에 인터넷을 교란시키려는 해커들에 의해 악용될 수 있다. 분산 서비스 거부 공격은 IP 패킷에 근원지 IP 주소를 스푸핑

하여 공격하기 때문에 공격경로와 패킷의 경로는 서로 다르다.



(그림 1) DDoS 공격 구조

[그림 2]는 분산 서비스 공격의 경우 공격경로와 패킷의 경로가 서로 다르다는 것을 보여주고 있다[2].



(그림 2) 패킷의 전송경로와 공격경로

2.2 IP 역추적

대부분의 DDoS 공격은 해커의 위치를 숨기기 위해서 IP 주소를 변경하여 공격을 시도한다. 이러한 공격에 대응하기 위해서는 우선적으로 해커의 실제 위치를 찾아 대응하는 방법이 필요하며, 이를 위해서 해커의 공격 패킷으로부터 별도의 부가적인 정보를 수집하여 공격 패킷의 실제적인 주소를 찾는 것을 IP 역추적 기술이라 불리며 4가지 기법이 존재한다. 먼저 역추적 마킹 기법(Traceback Marking) 기법으로 이는 패킷이 라우터를 거쳐갈 때, 라우터에서 자신의 특정 정보를 덧붙이고, 피해 시스템은 라우터 정보가 포함된 수신 패킷들을 통해 역추적하는 기법이다. 두 번째로 역추적 로깅 기법(Traceback Logging)기법은 라우터로 하여금 일정 기간 동안 키 라우터를 거쳐가는 모든 패킷 정보를 기록하여, 데이터 마이닝 기법을 이용하여 패킷을 역추적하는 기법이다. 세 번째는 링트 테스팅(Link Testing)기법으로 공격이 이루어지고 있는 동안 피해 시스템에 가장 가까운 라우터에서 시작하여 전달되는 패킷의 위치를 거슬러 올라가는 기법이다. 마지막으로 ICMP 역추적 기법(ICMP Traceback)은 라우터에 거쳐가는 패킷에 대해서 패킷의 일부가 포함된 ICMP 역추적 패킷을 생성하여 목적지 주소로 전송하고, 전송 받은 시스템은 해당 정보를 수집하여, 공격이 검출되면 수집된 정보를 이용하여 해커를 역추적 하는 기법이다[3].

2.3 역추적 시스템

2.3.1 호스트 기반 역추적 시스템(Host-based Traceback)

호스트 기반의 역추적 시스템은 인터넷 상에 설치된 모든 시스템에 역추적 모듈을 설치해야만 한다. 설치된 역추적 모듈을 이용하여 접속을 요구하는 시스템의 인증을 통해 역추적을 수행하거나,. 해당 시스템 내에 존재하는 각종 로그 기록을 분석하여 역추적을 수행하게 된다. 주요 역추적 기법으로는 AIAA가 있다.

AIAA(Autonomous Intrusion Analysis Agent) 시스템은 침해를 당한 서버의 해킹 피해 분석과 추적을 위한 로그 분석을 에이전트를 이용해 자동화한 역추적 시스템이다.AIAA 시스템은 침입자가 거쳐온 경유 시스템의 관리자의 도움을 받아 AIAA를설치하고, 이 시스템에서 바로 이전의 침입경로와 해킹 흔적을 분석하고 다시 이전의 침입시스템으로 분석을 옮겨가서 최종 경유지 서버까지 거슬러 간다.

AIAA 시스템은 역추적 경로상에 존재하는 시스템들의 관리자의 도움을 받아 설치하기 때문에 역추적을 완료하기까지 많은 시간이 필요하게 된다. 또한 역추적 경로상에 존재하는 모든 시스템에 직접 접속해야 하기 때문에 만약 관리자와의 협조가 불가능하여 시스템으로의 접근이 불가능한 경우 역추적 자체가 불가능할 수도 있다[4].

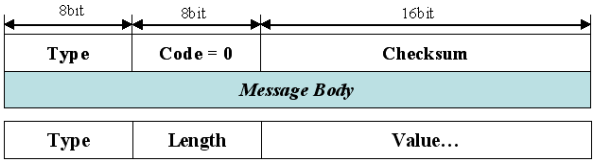
2.3.2 네트워크 기반 역추적 시스템 (Network-based Traceback)

네트워크 상에 송수신되는 패킷으로부터 정보를 추출하여 역추적을 수행하게 된다. 네트워크 기반 역추적 시스템은 송수신 패킷을 감시할 수 있는 위치에 역추적 모듈을 설치하게 된다. 주요 역추적 기법으로는 Thumbprints based algorithm이 있다.

Thumbprint란 말 그대로 지문을 의미한다. Thumbprint를 이용하는 방법은 역추적 시스템 전체를 의미하는 것이 아니라 역추적을 위해 공격자의 시스템으로부터 공격 대상 시스템까지의 연결 체인을 구성하는 알고리듬이다. 본 알고리듬은 연결 체인에 속하는 호스트들이 속한 네트워크 상에 송수신되는 데이터를 수집하여 비교한다. 그러나 패킷이 암호화되거나 터널링되어 패킷의 내용이 변경되는 경우, 해당 연결 체인을 구성할 수 없는 경우가 발생할 수 있다[4].

3. 역추적 시스템 설계

iTrace 메시지(ICMP Traceback Message)는 ICMP 패킷의 Message Body에 일련의 스트링으로 포함된다. ICMP Traceback Message를 위한 ICMP Type은 현재 정의되지 않았지만, IANA에서 조만간 정의 할 예정이다. Code 필드는 항상 '0' 으로 설정되며, Message Body는 하나의 이상의 TLV (Type-Length-Value) 엔트리로 구성된다. [그림 3]은 ICMP 역추적 메시지 형태를 보여주고 있다[5][6].



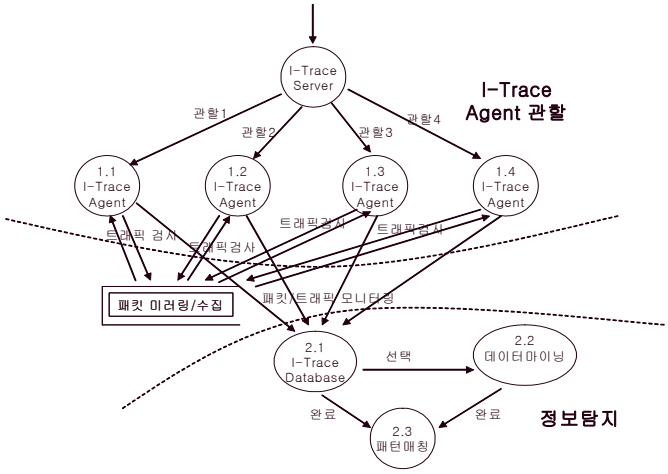
(그림 3) ICMP Traceback Message 형태

3.1 에이전트 시스템 설계

에이전트 시스템은 특정 IP에서 비정상 트래픽 현상이 발생하면 해당 IP를 감시하고, 발생시 문제 시스템을 손쉽게 찾아 해당 시스템의 정보와 수상한 Source IP를 서버에 신고하게 된다.

3.4 서버 시스템 설계

서버 시스템은 I-Trace 에이전트가 설치된 네트워크 전체를 아래 그림처럼 관할하고 통제할 수 있도록 구현되었다. 또한 I-Trace 서버의 메인 프로그램은 사용자에게 관할하는 네트워크의 현황을 실시간으로 모니터링 해주는 기능을 제공하도록 구현되었으며, 각 에이전트들은 자신이 가진 네트워크 관리 정보를 서버와 통신을 통해 교환하면서 유기적인 공격탐지 및 대응 프로세스를 처리하도록 개발 하였다.

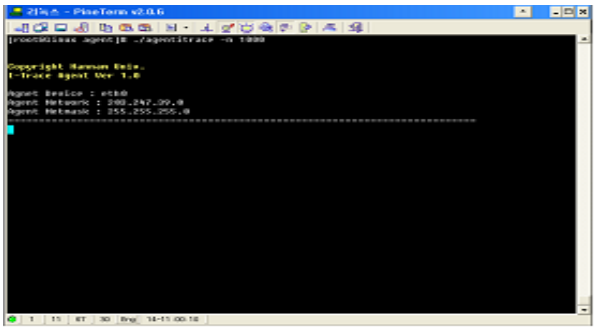


(그림 4) I-Trace System 구성 예시

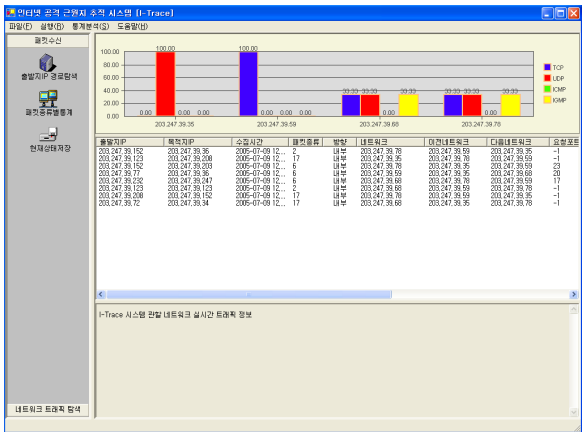
4. 네트워크 모니터링 및 공격자 역추적

4.1 네트워크 모니터링

에이전트 시스템에서는 관리자가 설정한 네트워크 임계치에 따른 패킷 수집을 제공하며, 패킷 헤더 정보를 iTrace 메시지 생성 모듈에 전송하게 된다. [그림 5]은 에이전트 시스템에서 임계치를 설정한 모습을 보여주고 있다. 그리고 [그림 6]은 패킷 모니터링을 보여주고 있다.

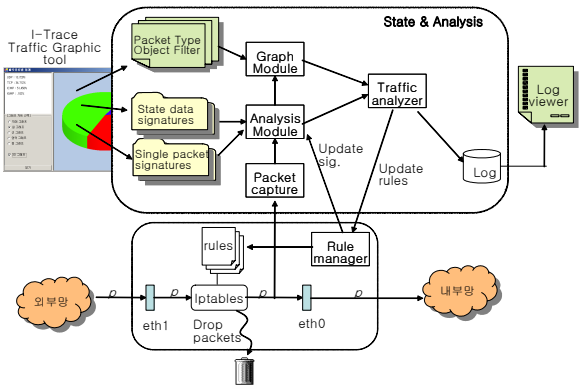


(그림 5) 임계치 설정 화면



(그림 6) 네트워크 모니터링

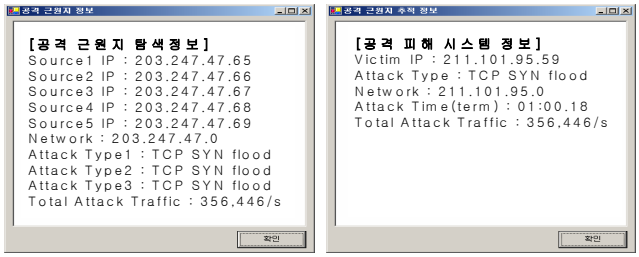
그리고 [그림 7]은 다양한 원시 데이터의 분석 단계별 과정을 거쳐 최대한 효율적인 가공을 통해 얻어지는 과정을 보여주고 있다.



(그림 7) 트래픽 통계 모듈 작업

4.2 공격 경로 재구성

에이전트 시스템들은 서버로부터 통보된 공격 패킷정보를 기반으로 공격패킷으로 의심되는 패킷들을 검사해 해당 공격 유형과 일치하는 패킷을 찾아낸다. 이렇게 일치하는 추적정보들을 모아서 Victim IP를 기준으로 정렬하고, 라우터에서 라우팅 테이블이 갱신되는 시간 간격을 갖도록 앞서 정렬된 추적정보를 시간에 따라서 그룹화를 한다. 그런 다음 각 그룹에 속하는 데이터별로 라우터(에이전트) 주소, 패킷이 유입된 인터페이스 등의 정보를 갖는 역추적 노드를 생성한다. 이런 과정을 각 네트워크에서 반복하여 최종적인 공격경로의 재구성이 이루어지게 된다.



(그림 8)Attacker와 Victim 정보화면

5. 결론 및 향후 연구 방향

인터넷 사용자의 급속한 증가로 인한 복잡한 TCP 반응과 연관되어 네트워크 서비스에 많은 패킷 손실을 야기하게 되었다. 이러한 문제를 해결하기 위하여 대학 연구소와 기업체에서는 침입대응 시스템을 개발하게 되었고, 공격자의 근원지를 추적하는 역추적 시스템이 등장하게 되었다. 따라서 본 논문에서는 이러한 침입에 대한 대응을 위해 ICMP 기반의 역추적 시스템을 분석 및 설계하였다. 향후 연구로는 세밀한 분석을 통하여 모듈을 설계하고, 이 설계를 바탕으로 역추적 Agent와 역추적 Manager를 구현하고자 한다. ICMP 역추적 메시지는 현재 IETF internet Area의 itrace Working Group에서 Internet draft로 제출된 상태이다. ICMP 역추적 기법은 라우터에 거쳐가는 패킷에 대해서 패킷의 일부가 포함된 ICMP 역추적 패킷을 생성하고 목적지 주소로 전송하고, 전송 받은 시스템은 해당 정보를 수집하여, 공격이 검출되면 수집된 정보를 이용하여 해커를 역추적 하는 기법이다. 더 나아가 이를 능동 네트워크 기반으로 발전시켜 새로운 역추적 시스템을 구현하고자 한다.

참고문헌

[1] 이만영, 손승원, 조현숙, 정태명, 채기준 "차세대 네트워크 보안 기술" 생능출판사, pp.415-430, 2002.11.25

[2] 이형우, "DDoS 해킹 공격 근원지 역추적 기술" 정보보호학회지, 2003.10

[3] 강호호외 3명, "IP 역추적 기술 동향", 주간기술동향, 97-39 한국전자통신연구원

[4] S. Savage, D. Wetherall, A. karlin, and T. Anderson, "Network Support for IP Traceback", IEEE/ACM transactions on networking, vol. 9, No. 3, June 2001.

[5] Steve Bellovin외 2명, “ICMP Traceback Messages”, Internet Draft, IETF, Feb. 2003.

[6] Allison Mankin외 4명, “On Design and Evaluation of Intention-Driven ICMP Traceback”

[7] “차세대 인터넷을 위한 능동 보안 기술 백서”, 한국전자통신연구원